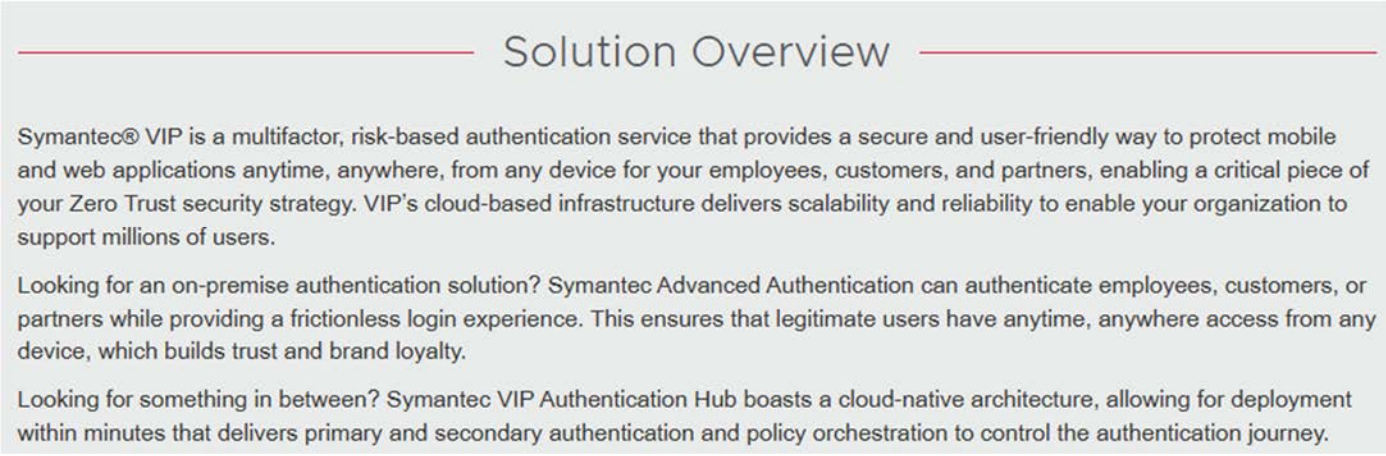
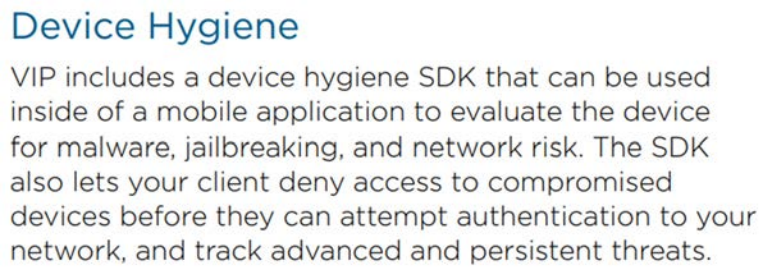
UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

QUICKVAULT, INC., Plaintiff, v. BROADCOM INC., d/b/a BROADCOM CORPORATION Defendant.	Case No.: 1:24-cv-00864 **JURY TRIAL DEMANDED**

EXHIBIT M

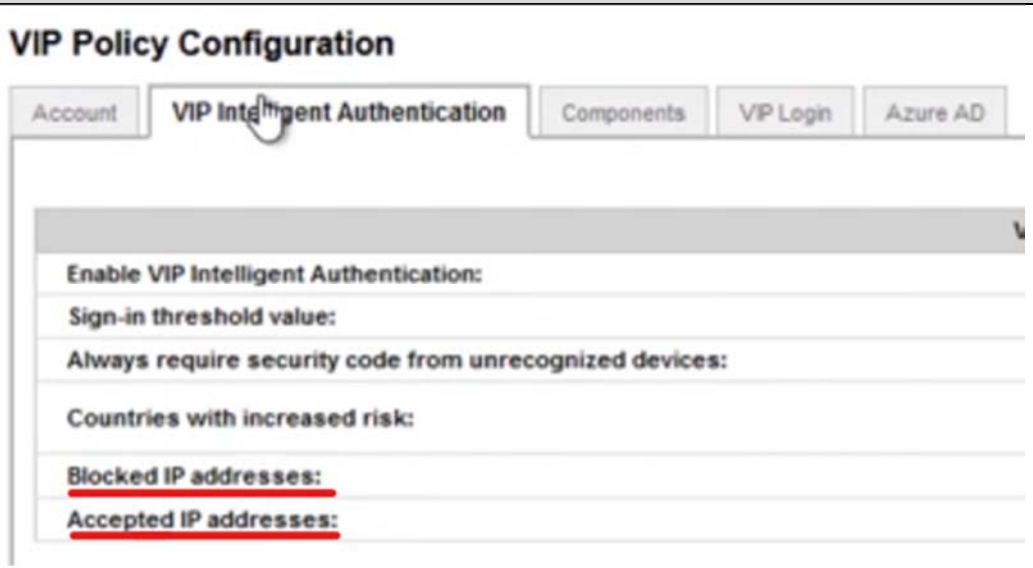
’437 Patent Infringement Claim Chart

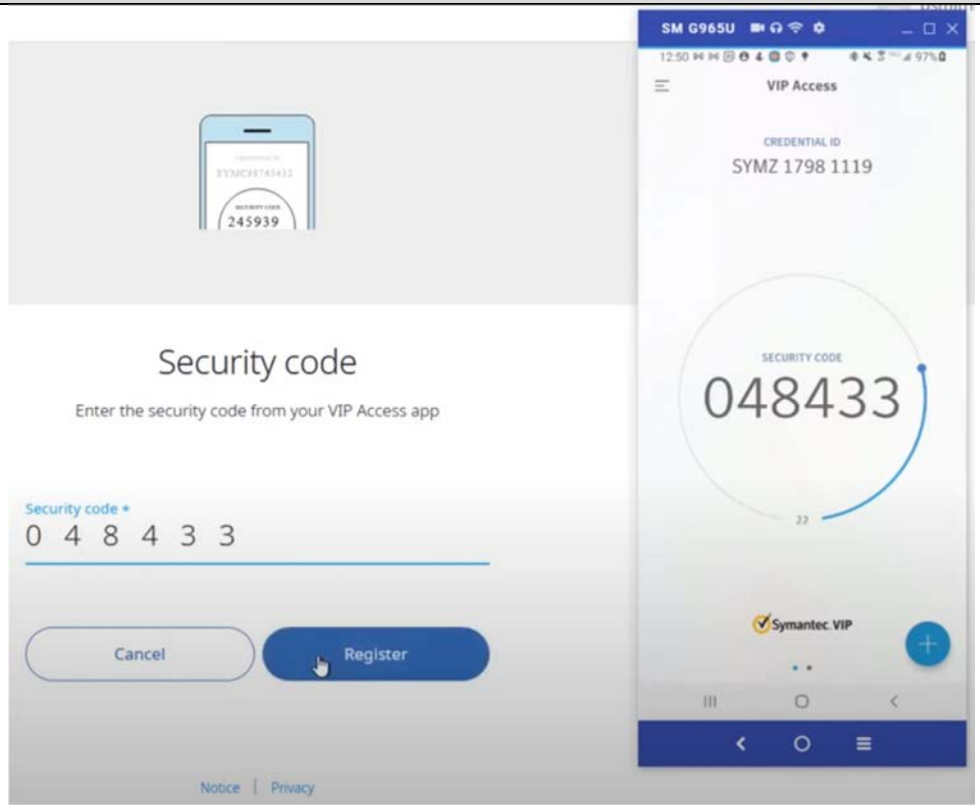
EXHIBIT M: U.S. PATENT NO. 11,880,437 INFRINGEMENT CLAIM CHART[1]

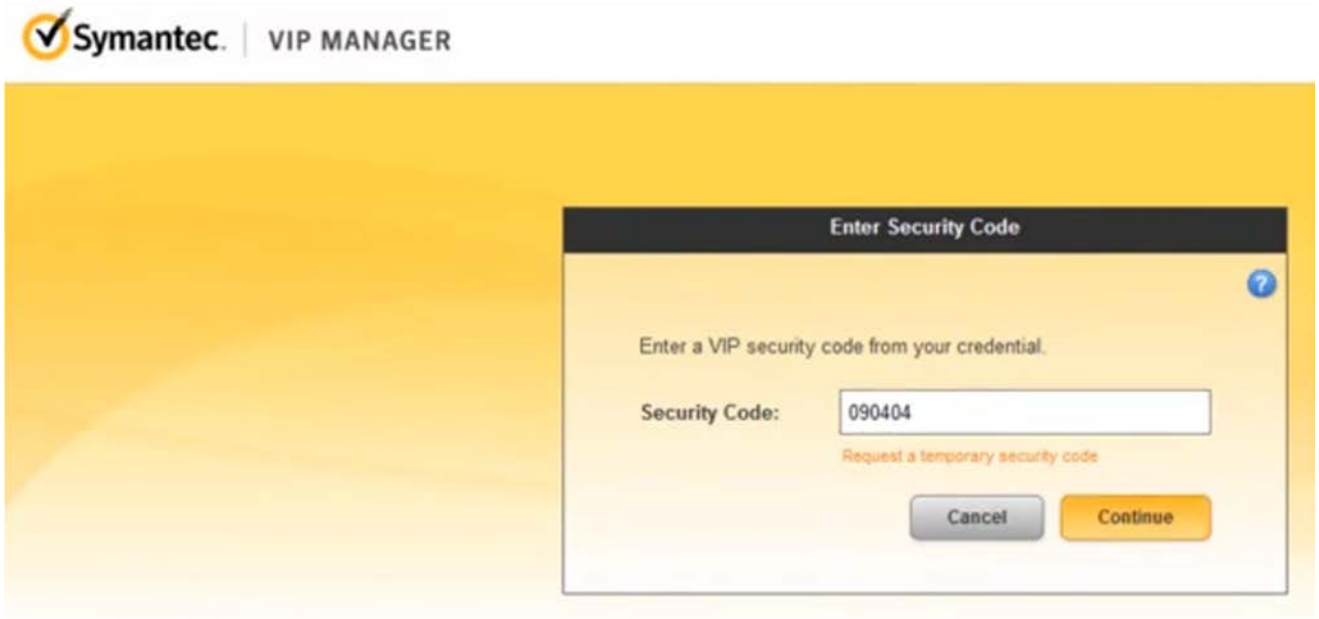
Claim 1	Broadcom Symantec VIP
A computer-implemented method for remote data access using a user device, the computer-implemented method comprising:	The preamble is presumptively not limiting. To the extent the preamble is limiting, Symantec VIP performs a computer-implemented method for remote data access using a user device.  Solution Overview Symantec® VIP is a multifactor, risk-based authentication service that provides a secure and user-friendly way to protect mobile and web applications anytime, anywhere, from any device for your employees, customers, and partners, enabling a critical piece of your Zero Trust security strategy. VIP's cloud-based infrastructure delivers scalability and reliability to enable your organization to support millions of users. Looking for an on-premise authentication solution? Symantec Advanced Authentication can authenticate employees, customers, or partners while providing a frictionless login experience. This ensures that legitimate users have anytime, anywhere access from any device, which builds trust and brand loyalty. Looking for something in between? Symantec VIP Authentication Hub boasts a cloud-native architecture, allowing for deployment within minutes that delivers primary and secondary authentication and policy orchestration to control the authentication journey. (https://www.broadcom.com/products/identity/vip)
receiving, by a remote computer from the user device, an authentication request comprising a user device unique	 Device Hygiene VIP includes a device hygiene SDK that can be used inside of a mobile application to evaluate the device for malware, jailbreaking, and network risk. The SDK also lets your client deny access to compromised devices before they can attempt authentication to your network, and track advanced and persistent threats.

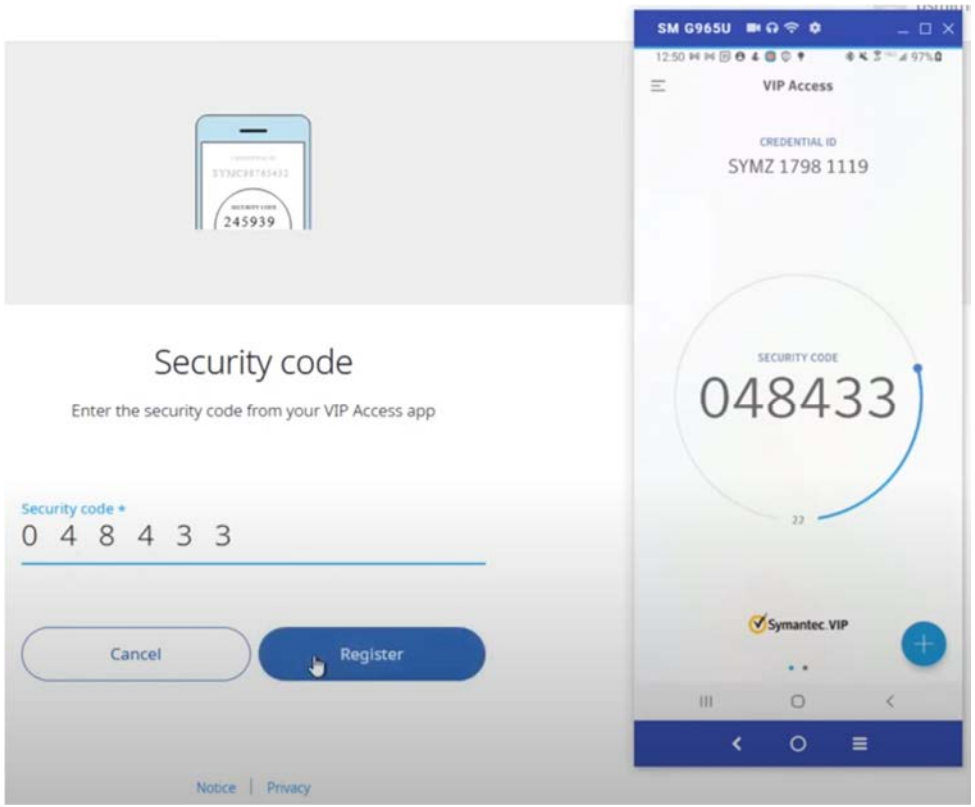
[1] The evidence of infringement identified in the below chart is exemplary and nonlimiting. QuickVault reserves the right to rely on additional and/or alternative aspects of Symantec VIP and related components during this litigation for the purpose of establishing infringement.

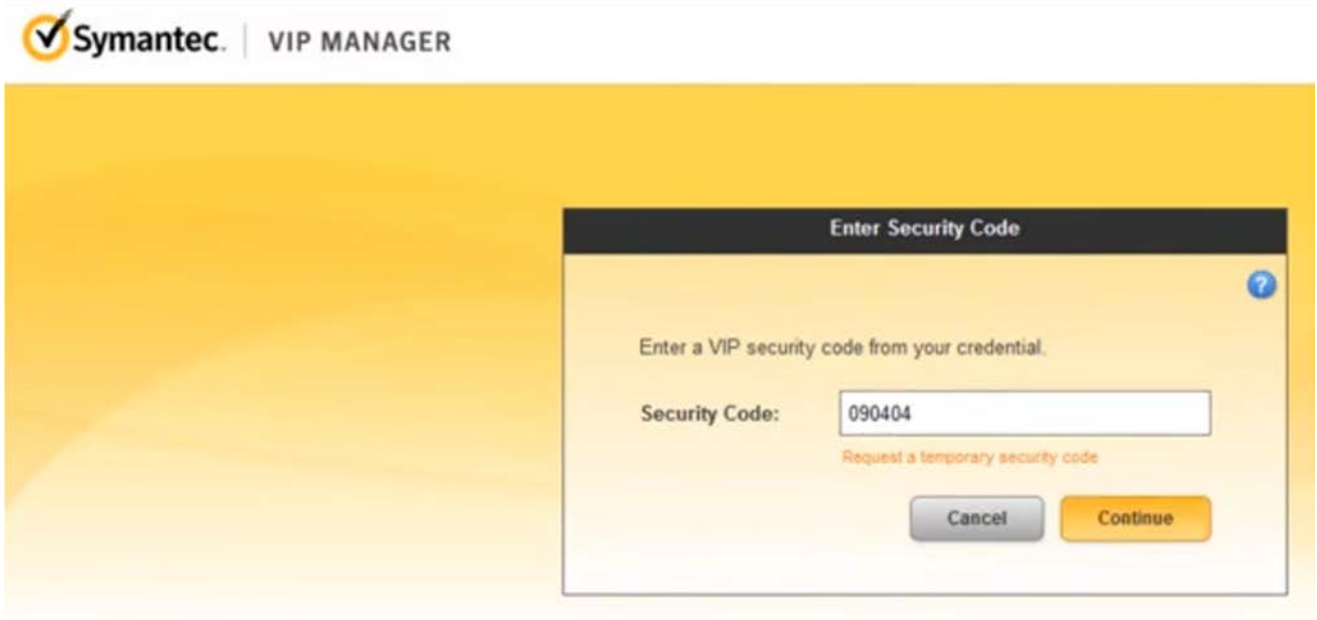
Claim 1	Broadcom Symantec VIP
identifier and a mobile authentication device unique identifier,	Multifactor Authentication Being able to positively identify legitimate users from fraudulent ones is an important first step to achieving Zero Trust, and a critical step in designing a modern identity fabric. VIP enables enterprises to deliver secure access to corporate networks and applications from anywhere in the world, providing improved productivity and better insight. The service offers a multitude of user-friendly authentication options to protect against unauthorized access, including a broad range of second-factor options such as push, SMS or Voice OTP, mobile authenticators, FIDO2, and biometrics. VIP also offers a series of hardware-based authenticators, including cards, keys, and tokens that can be purchased separately. These options can be used for internal employees or partners. Finally, the cloud-based service is also built to protect consumer-facing mobile and web applications, resulting in increased customer confidence and reduced fraud costs. (https://docs.broadcom.com/doc/symantec-vip)

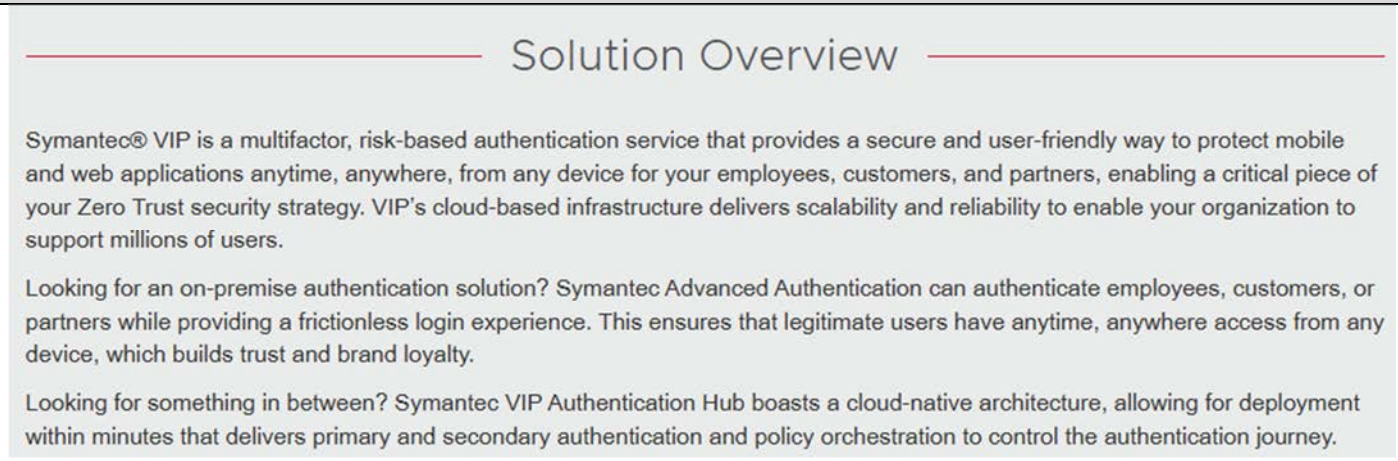
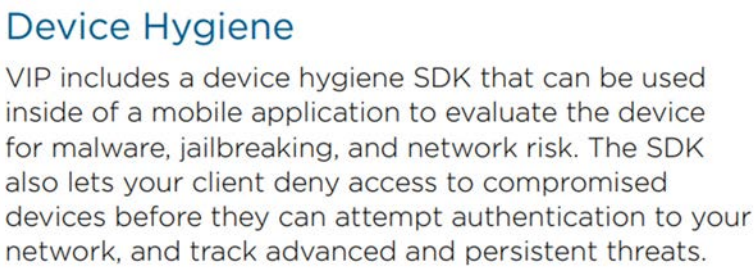
Claim 1	Broadcom Symantec VIP
	 (https://www.youtube.com/watch?v=SdY13B5mExI (5:47))

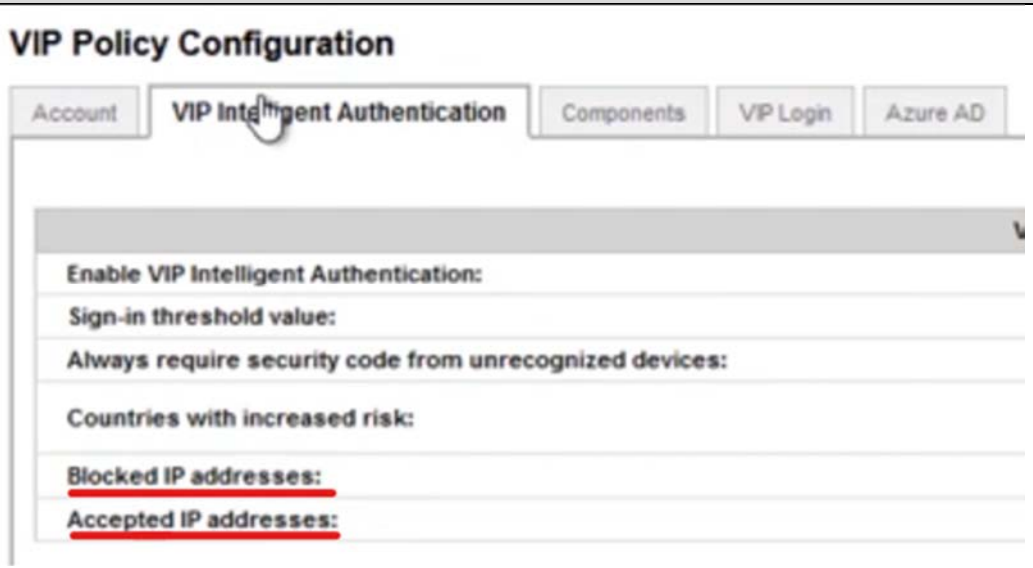
Claim 1	Broadcom Symantec VIP
	 (https://www.youtube.com/watch?v=SdY13B5mExI (1:33))

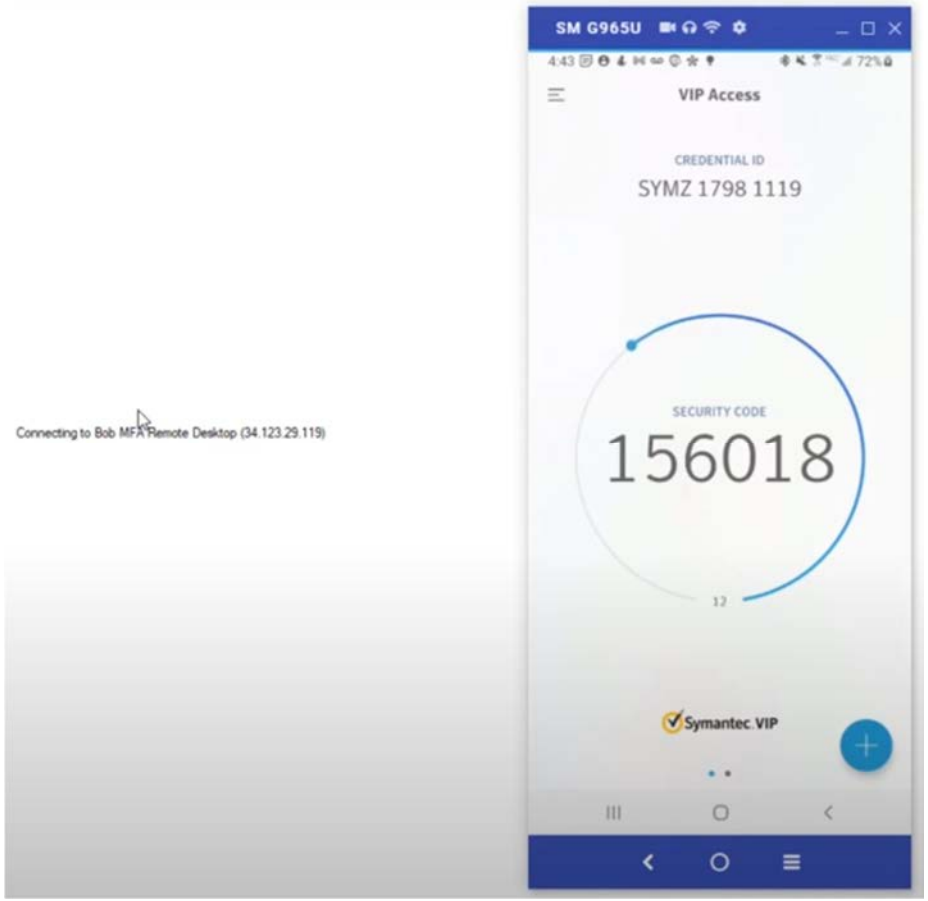
Claim 1	Broadcom Symantec VIP
	 (https://www.youtube.com/watch?v=SdY13B5mExI (3:30))

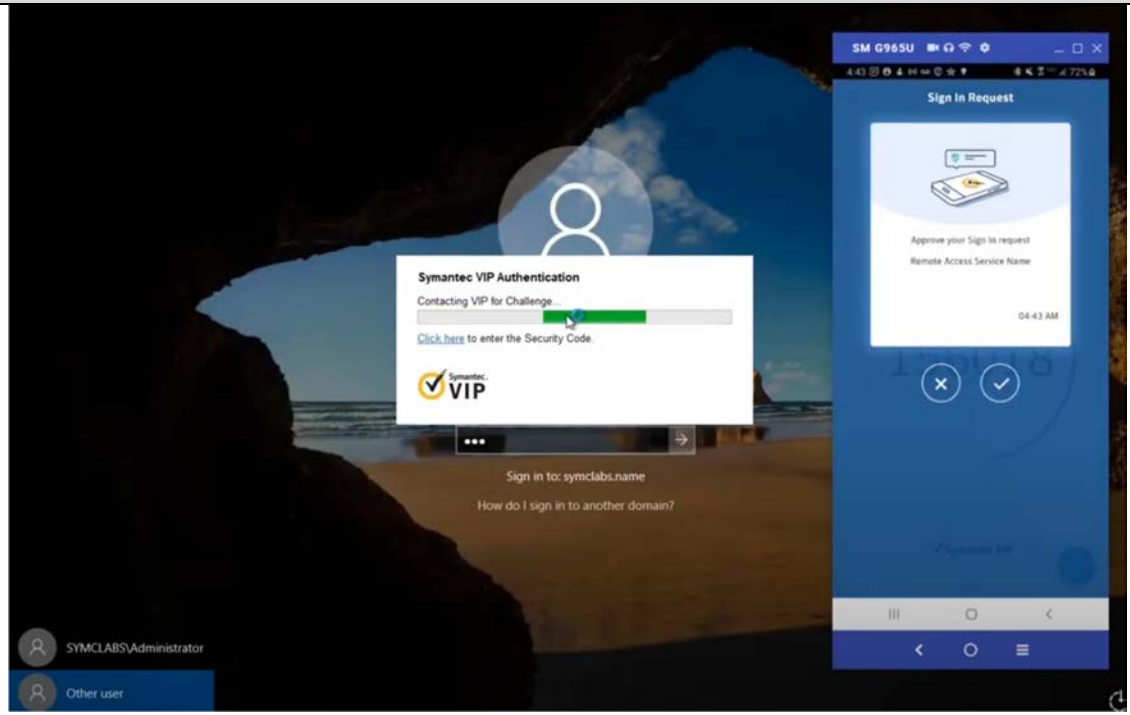
Claim 1	Broadcom Symantec VIP
wherein the mobile authentication device unique identifier is provided to the user device from a mobile authentication device, and	 (https://www.youtube.com/watch?v=SdY13B5mExI (1:33))

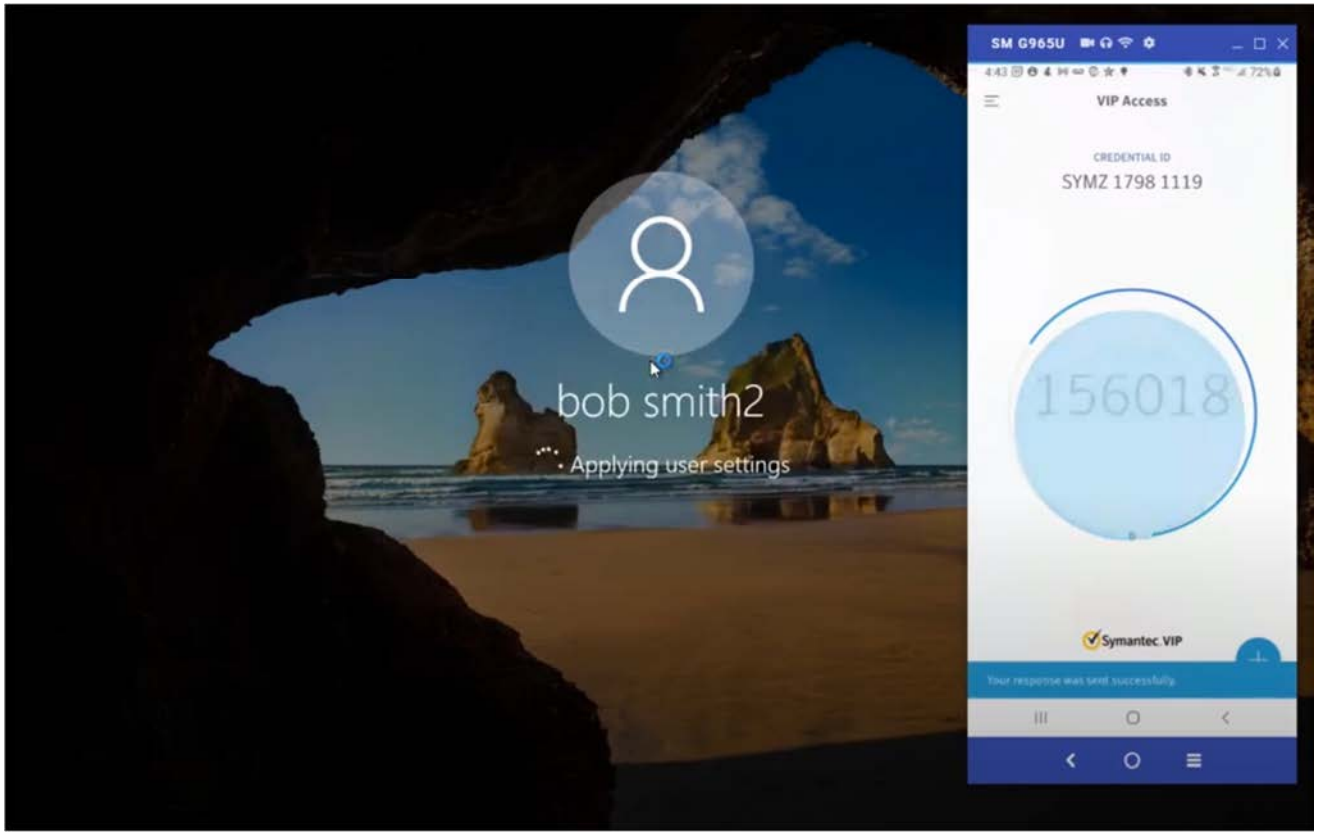
Claim 1	Broadcom Symantec VIP
	 (https://www.youtube.com/watch?v=SdY13B5mExI (3:30))
wherein the mobile authentication device and the user device are associated with a software license stored on the remote computer;	The mobile authentication device and the user device are associated with a software license to at least Symantec VIP stored on the remote computer.

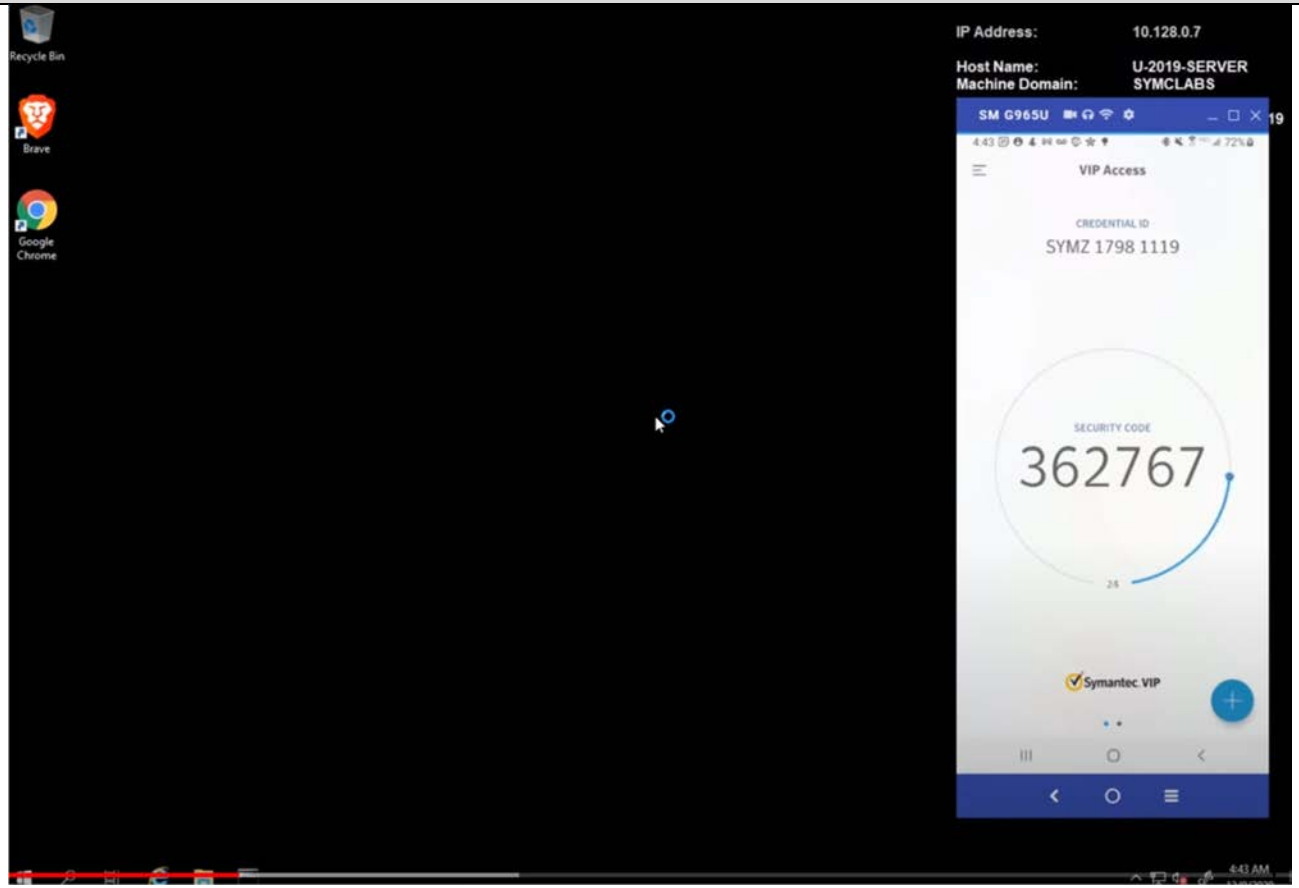
Claim 1	Broadcom Symantec VIP
	 (https://www.broadcom.com/products/identity/vip)
determining, by the remote computer, that the user device is authorized for use with the software license by determining that the user device unique identifier is valid in combination with the software license stored on the remote computer;	 (https://docs.broadcom.com/doc/symantec-vip)

Claim 1	Broadcom Symantec VIP
	 (https://www.youtube.com/watch?v=SdY13B5mExI (5:47))

Claim 1	Broadcom Symantec VIP
upon determining, by the remote computer, that the user device is authorized for use with the software license, transmitting, by the remote computer to the user device, a validation message associated with the user device; and	 (https://www.youtube.com/watch?v=SdY13B5mExI (2:35))

Claim 1	Broadcom Symantec VIP
	 (https://www.youtube.com/watch?v=SdY13B5mExI (2:39))

Claim 1	Broadcom Symantec VIP
responsive to transmitting the validation message, transmitting, by the remote computer, data to the user device.	 (https://www.youtube.com/watch?v=SdY13B5mExI (2:45))

Claim 1	Broadcom Symantec VIP
	 (https://www.youtube.com/watch?v=SdY13B5mExI (2:54))